BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

WHAT IS CLAIMED IS:

1. A system for reducing payments risk, liquidity risk and systemic risk associated with payments-based transactions, said system comprising:

a communications network formed by the interlinking of a plurality of internet protocol (IP) networks;

a plurality of User Host Applications supported over said communications network for use by plurality of Users active in payments-based transactions;

a plurality of Third Party Host Applications supported over said communications network for use by plurality of Third Parties active in payments-based transactions; and

a plurality of Payment Bank Host Applications supported over said communications network for use by a plurality of Payment Banks operating a plurality of domestic payment systems, each said Payment Bank Host Application having means for processing payment messages, including payments instructions to be carried out in said domestic payments system on behalf of a plurality of account holders (including bank correspondents), and

wherein each said Payment Bank Host Application includes a filter process module for automated processing of said payments instructions based on (i) payments risk parameters and (ii) the accounts of said Users (User accounts) such that payments instructions breaching said payments risk parameters are rejected back to a payments processing queue for later re-evaluation, thereby reducing payments risk, liquidity risk and systemic risk throughout said system.

2. The system of claim 1, wherein each Third Party Host Application, said User Host Application and said Payment Bank Host Application sends payments risk data and generates and receives payments-related notifications, inquiries, messages and reports via their respective host applications.

3. The system of claim 1, wherein said Filter Process Module in each said Payment Bank Host Application is integrated with payments processing such that payments instructions are filtered for compliance using suspend payment instructions and said payments risk parameters.

4. The system of claim 1, wherein each said Third Party Host Application and said User Host Application can request and receive multi-currency reports from said plurality of Payment Bank Host Applications.

5. The system of claim 1, wherein each said Payment Bank Host Application is capable of calculating the Available Balance for counterparty payments using data interchange with existing payments confirmation services and monitoring elapsed time.

6. The system of claim 5, wherein each said Payment Bank Host Application can generate a notification to the Payment Bank and User and/or Third Party in the event that a counterparty fails to make expected payments for a pre-determined period of elapsed time.

7. The system of claim 6, wherein each Third Party or User receiving notification of a counterparty payment failure may instruct Payment Bank to suspend further payments to said counterparty.

8. The system of claim 6, wherein each said Payment Bank Host Application automatically incorporates a suspension of all further payments to a counterparty on receipt of a notification to do so via implementation as a trigger in said Filter Process Module.

9. The system of claim 1, wherein each Payment Bank and User use digital certification to establish their access authority and usage constraints, and wherein data transmissions over said communication network are encrypted for security purposes.

10. The system of claim 1, wherein said Third Party, User and Payment Bank Host Applications are human-accessible by browser interface and machine-accessible by incorporation and translation of electronic data interchange formats.

11. The system of claim 1, wherein Third Parties and Users can flexibly identify counterparties by means of aggregating identifiers unique to individual corporate or organizational entities, creating thereby synthetic counterparties composed of entities deemed to share correlation in payment risk assessment.

12. The system of claim 1, which further comprises a processor-based Core System being operably connected to said global communications network and supporting a Core System Host Application, wherein said Core System Host Application comprises information storage means for recording various type of information, including identification of said Users, identification of said Third Parties, identification of said Payment Banks, identification of said counterparties, identification of currencies, specification of the Clean Payment Limit (Debit Cap), and Payment Type identification (including alternative payment channels, if any).

13. A method of reducing payments risk, liquidity risk, and systemic risk in a system supporting a plurality of Third Party Host Applications, a plurality of User Host Applications, and a plurality of Payment Bank Host Applications, each said payment Bank Host Application has a Filter Process Module for processing payments instructions, said method comprising the steps:

(a) said Third Parties sending counterparty payments risk data to said Users associated with a plurality of payments-based transactions;

(b) said Users sending counterparty payments risk data on behalf of themselves and said Third Parties to said system, wherein said payments risk data specifies transaction parameters selected from the group consisting of

(i) the User associated with each said payments-based transaction,

(ii) the Third Party (if any) associated with each said payments-based transaction,

(iii) the Payment Bank associated with each said payments-based transaction,

(iv) the counterparty associated with each said payments-based transaction,

(v) the currency associated with each said payments-based transaction,

(vi) the payment type associated with each said payments-based transaction, and

(vii) the Clean Payment Limit associated with each said payments-based transaction;

(c) said system analysing the payments risk data associated with each said payments-based transaction and decomposing said payments risk data into files for transfer to said Payment Bank Host Applications making payments on behalf of said Users in a plurality of currencies;

(d) said system transmitting said payments risk data, associated with each said payments-based transaction, to said Payment Bank Host Applications, using application-to-application automated interfaces; and

(e) each said Payment Bank Host Application applying said payments risk data as input parameters to said Filter Process Module for automated evaluation of payments instructions in respect of accounts of said Users (User accounts) such that payments instructions breaching said input parameters to said Filter Process Module are rejected back to a payments processing queue for later re-evaluation.

14. The method of claim 13, wherein each Third Party, User and Payment Bank sending payments risk data can also generate and receive payments-related notifications, inquiries, messages and reports via their respective host applications.

15. The method of claim 13, wherein said Filter Process Module within each said Payment Bank Host Application cooperates with payments processing with said domestic payment system operated by said Payment Bank, such that payments instructions are filtered by said Filter Process Module for compliance with suspend instructions and payment risk parameters.

16. The method in claim 14, wherein each Third Party and User can request and receive multi-currency reports from a plurality of said Payment Banks acting on their behalf.

17. The method of claim 13, wherein each said Payment Bank Host Application capable of calculating the Available Balance for counterparty payments through incorporation of data interchange with existing payments confirmation services and monitoring elapsed time.

18. The method of claim 14, wherein each Payment Bank Host Application can generate a notification to the Payment Bank and User and/or Third Party in the event that a counterparty fails to make expected payments for a pre-determined period of elapsed time.

19. The method of claim 18, wherein each Third Party or User receiving notification of a counterparty payment failure may instruct Payment Bank suspension of further payments to said counterparty.

20. The method of claim 17, wherein each Payment Bank Host Application will automatically incorporate a suspension of all further payments to a counterparty on receipt of a notification to do so via implementation as a trigger in the Filter Process Module.

21. The method of claim 13, wherein each Payment Bank and User are subjected to digital certification to establish their access authority and usage constraints, and wherein data transmissions are encrypted for security purposes.

22. The method of claim 13, wherein Third Party, User and Payment Bank host applications are human-accessible by browser interface and machine-accessible by incorporation and translation of electronic data interchange formats.

23. The method of claim 13, wherein Third Parties and Users can flexibly identify counterparties by means of aggregating identifiers unique to individual corporate or organizational entities, creating thereby synthetic counterparties composed of entities deemed to share correlation in payment risk assessment.

24. The method of claim 13, wherein said system further comprises Core System Host Application for recording various type of information, including identification of said Users, identification of said Third Parties, identification of said Payment Banks, identification of said counterparties, identification of currencies, specification of the Clean Payment Limit (Debit Cap), and Payment Type identification (including alternative payment channels, if any).

25. A global computer-based system for mitigating risk arising in connection with foreign exchange settlements and other payments between financial market participants, wherein a mechanism is provided for efficiently controlling payments risk in as many currencies as may be interoperable with said system.

26. A computer-based payment risk management system, wherein a mechanism is provided for controlling payment flows within a single domestic payment system and globally through a multi-currency implementation so that payment risk is reduced between counterparties.

27. A computer-based payment risk management system, wherein a mechanism is provided for reducing payments risk arising for an account holder within a single currency, as well as cross-border payments risk arising from payments in a plurality of currencies.

28. A computer-based payment risk management system, wherein a mechanism is provided for controlling payments risk for all payment flows, whether arising from foreign exchange transactions or other payment types.

29. A computer-based payment risk management system, wherein a mechanism is provided for enabling a participant to unilaterally control his risk vis-a-vis a particular payments counterparty, without the necessity for the counterparty's agreement or cooperation.

30. A computer-based payment risk management system, wherein a mechanism is provided for allowing participants to more efficiently manage their current business, reduce overhead, improve returns on capital, and support new business with counterparties by reducing payments risk and enabling more efficient liquidity and credit risk management.

31. An Internet-based computer-based system, wherein separate accounts can be flexibly aggregated or disaggregated by participants for risk management and reporting purposes to promote effective oversight of group or individual participant use of the system.

32. An Internet-based computer-based system, wherein separate counterparty accounts can be flexibly aggregated or disaggregated for risk management purposes and reporting purposes according to participant

assessment of risk correlation between affiliated, connected or similar counterparties.

33. A computer-based system, wherein payment flows with a counterparty or counterparties in a plurality of currencies can be flexibly aggregated for risk management purposes and reporting purposes.

34. A computer-based payments risk reduction system that is consistent with and complementary to the existing network for inter-bank financial communications (S.W.I.F.T.) and the internet protocol networks increasingly used by financial institutions.

35. A computer-based payments risk reduction system which allows individual participants to determine unilaterally their tolerances for payment risk according to counterparty, currency and payment type.

36. A computer-based payments risk reduction system, wherein participants can view, enter and alter their risk parameters for counterparties, currencies and payment types on a real-time basis.

37. A computer-based payments risk reduction system, wherein the payment parameters of account holders can be entered into the database of the system by way of screen-entry, batch-entry or integration with internal systems processes.

38. A computer-based payments risk reduction system, wherein payments risk can be controlled in an automated manner through integration with the existing payments systems operating within payment banks directly connected to domestic payments systems.

39. A computer-based payments risk reduction system, wherein a mechanism is provided for enabling payment banks to integrate the system host application in a modular fashion in connection with their participation in domestic payment systems with a high degree of openness, flexibility and interoperability.

40. A computer-based payments risk reduction, wherein a mechanism is provided for monitoring payment flows and reporting exception situations which may indicate a counterparty payment failure.

41. A computer-based payments risk reduction system for use by a payment bank, wherein a mechanism is provided for notifying account holders of payment problems intra-day, enabling them to take such actions as will forestall any adverse impact on liquidity in that and other currencies.

42. A computer-based payments risk reduction system, wherein a mechanism is provided for inquiring into exception situations between

participants, counterparties and payment banks, and facilitating earlier corrective action or remedial action as appropriate.

43. A computer-based payments risk reduction, wherein account holders can notify payment banks in real-time of their wish to suspend any further payments to an individual counterparty.

44. A computer-based payments risk reduction system for use within a payment bank, having a mechanism for efficiently and effectively suspending any further payments to a particular counterparty on behalf of an account holder, following receipt of a request from an account holder to do so.

45. A computer-based system enabling automated calculation of global risk positions based on payments activities in multiple payments systems.

46. The computer-based system of claim 45, wherein the advantages of Web-based information management, browser interfaces, application-to-application data interchange, object-oriented programming and open systems technologies are integrated to deliver improved flexibility, extensibility, modularity, interoperability and other information management advantages in connection with payments risk management.

47. A computer-based system, wherein a mechanism is provided for reducing the systemic risk that a payment failure by one market counterparty

may lead to failure of contingent payments down a chain of interrelated payments transactions, and thereby threaten the liquidity and integrity of payment and banking systems within a single market or globally.

48. The computer-based system of claim 47, wherein a participant's payments liquidity is optimally used to meet payment obligations in an automated manner.

49. The computer-based system of claim 47, wherein liquidity management software is employed to address cross-border payment risk or payment risk arising on the level of the individual account holder within a participating bank.

50. The computer based system of claim 47, wherein payment instructions can be processed very rapidly after negotiation of the underlying transaction without compromising payments risk mitigation.

51. The computer-based system of claim 47, wherein means are provided for enabling access via a plurality of internet protocol networks and a plurality of computing devices, and flexibility in the use and configuration of access software to meet individual functional requirements and capacity to support technological integration.

52. The computer-based system of claim 47, wherein many-to-many data processing techniques are used to rationalise the flows of information between

host applications located anywhere around the globe (in both developed and emerging markets) without the prejudices and disadvantages arising from geographical dispersion.

53. The computer-based system of claim 47, wherein payment risk parameters and other data are entered into the system and automatically interpreted by rule-based interpretation procedures as to processing requirements.

54. The computer-based system of claim 47, wherein account holder payment parameters are managed on a database and communicated as operable parameters for payments processing by host applications in payment banks.

55. The computer-based system of claim 47, which uses or interoperates with industry standard data formats for the capture and transmission of like data to enable efficient interface with pre-existing banking applications and systems.

56. The computer-based system of claim 47, which provides appropriate security and integrity for the transmission of all data across its network via cryptographically secure sessions and digital certification of host application subscribers.